Amendment to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

Claim 1 (currently amended). A method of communicating private data between computers coupled to a data communication network, said computers including a first client and a second client coupled to the data communication network, said method comprising:

receiving, at a network server, a plurality of keys encrypted by the first client in response to a request from a user of the first client to roam a private ~~data~~ key, said plurality of keys including the private key, a wrapping key generated by the first client in response to an encryption password received from the user, and a recovery key generated by the first client, said private key being encrypted ~~by a first client~~ as a function of [[a]] said wrapping key, said wrapping key and said recovery key being unknown to the server, said server ~~and said first client~~ being coupled to the data communication network;

generating, at the server, a backup key in response to the plurality of encrypted keys received from the first client;

storing the received plurality of encrypted ~~private data~~ keys and the generated backup key at the server;

receiving, at the server, a request from [[a]] the second client for ~~the encrypted private~~ backup data; and

in response to the received request, transferring the encrypted ~~private data~~ recovery key and the backup key from the server to the second client, said second client generating a backup encrypted recovery key representative of the recovery key encrypted as a function of the transferred backup key for storage on the second client ~~for decryption as a function of the wrapping key~~.

Claim 2 (canceled).

Claim 3 (currently amended). The method of claim [[2]] 1, further comprising decrypting the encrypted ~~private~~ recovery key at the second client as a function of the wrapping key, said wrapping key being generated on the second client in response to the encryption password received from a user of the second client.

Claim 4 (currently amended). The method of claim ~~2, further comprising:~~ 1, wherein

~~receiving, at the server, the wrapping key encrypted by the first client as a function of a recovery key unknown to the server,~~ said recovery key ~~being~~ is generated on the first client in response to a recovery option selected by the user~~; and~~

~~receiving, at the server, the recovery key encrypted by the first client as a function of the wrapping key~~.

Claim 5 (canceled).

Claim 6 (currently amended). The method of claim [[5]] 1, further comprising transferring the encrypted private key and the encrypted wrapping key from the server to the ~~first~~ second client in response to ~~the~~ a received recovery request, said backup encrypted recovery key stored on the ~~first~~ second client being decrypted, at the ~~first~~ second client, as a function of the transferred backup key to obtain the recovery key, said encrypted wrapping key being decrypted, at the ~~first~~ second client, as a function of the obtained recovery key to obtain the wrapping key, and said encrypted private key being decrypted, at the ~~first~~ second client, as a function of the obtained wrapping key to obtain the private key.

Claim 7 (currently amended). The method of claim [[5]] 1, further comprising transferring the encrypted recovery key and the ~~transferred~~ backup key to the first ~~second~~ client in response to a backup request received from the user of the first ~~second~~ client, said transferred encrypted recovery key being decrypted, at the first ~~second~~ client, as a function of the wrapping key generated on the first ~~second~~ client to obtain the recovery key, said first ~~second~~ client encrypting

the obtained recovery key as a function of the transferred backup key to generate the backup encrypted recovery key for storage in a memory associated with the first ~~second~~ client.

Claim 8 (currently amended). The method of claim [[5]] 1, further comprising:

retrieving the stored backup key from the database associated with the server in response to a recovery request received from the user of the second client; and

transferring the backup key from the server to the second client in response to the received recovery request.

Claim 9 (currently amended). The method of claim [[5]] 7, further comprising transferring the encrypted private key and the encrypted wrapping key from the server to the first ~~second~~ client in response to a recovery request received from the first ~~second~~ client via the data communication network, said backup encrypted recovery key stored on the first ~~second~~ client being decrypted, at the first ~~second~~ client, as a function of the transferred backup key to obtain the recovery key, said encrypted wrapping key being decrypted, at the first ~~second~~ client, as a function of the obtained recovery key, and said encrypted private key being decrypted, at the first ~~second~~ client, as a function of the obtained wrapping key to obtain the private key.

Claim 10 (original). The method of claim 1 wherein the second client is a roaming client computer coupled to the data communication network.

Claim 11 (currently amended). One or more computer readable storage media having computer-executable instructions for performing the method of claim 1.

Claim 12 (currently amended). A system for communicating private data on a data communication network, comprising:

a first client coupled to the data communication network for receiving a request from a user to roam a private key and responding to said request, said responding by the first client comprising:

generating a wrapping key as a function of an encryption password provided by the user;

generating a recovery key;

encrypting the private key as a function of the wrapping key;

encrypting the wrapping key as a function of the recovery key; and

encrypting the recovery key as a function of the wrapping key;

a server for receiving the private, wrapping, and recovery keys ~~private data~~ encrypted by [[a]] the first client and in response to receiving said encrypted keys, generating a backup key ~~as a function of a wrapping key unknown to the server~~, said server ~~and said first client~~ being coupled to the data communication network;

a database associated with the server, said server being configured to store the received encrypted keys ~~private data~~ and the generated backup key in the database and to transfer backup data in response to receiving a request for the backup data, said backup data including the stored encrypted ~~private data~~ recovery key and the stored backup key; and ~~to a second client also coupled to the data communication network for decryption as a function of a wrapping key in response to a request for the encrypted private data received from the second client~~

a second client coupled to the data communication network for requesting the backup data from the server and generating a backup encrypted recovery key in response to receiving said backup data from the server, said generating by the second client comprising:

receiving the encryption password from the user;

decrypting the encrypted recovery key as a function of the received encryption password;

encrypting the backup key as a function the recovery key; and

storing the backup encrypted recover key in a memory associated with the second client.

Claim 13 (canceled).

Claim 14 (currently amended). The system of claim [[13]] 12, wherein the first client is configured to ~~generate the wrapping key on the first client, encrypt the private data as a function of the generated wrapping key, and generate a~~ store the generated recovery key ~~for storage~~ on the first client.

Claim 15 (canceled).

Claim 16 (canceled).

Claim 17 (currently amended). The system of claim 16 wherein the backup key is randomly generated by the server in response to receiving said plurality of encrypted keys ~~private data~~ from the first client.

Claim 18 (canceled).

Claim 19 (canceled).

Claim 20 (currently amended). The system of claim [[19]] 12 wherein the server is further configured to transfer the encrypted private key, the generated backup key, and the encrypted wrapping key to the second client computer in response to a recovery request received from the second client computer, wherein the ~~second~~ backup encrypted recovery key stored in the memory associated with the second client computer is decrypted, at the second client, as a function of the transferred backup key to obtain the recovery key, said transferred encrypted wrapping key being decrypted, at the second client, as a function of the obtained recovery key to obtain the wrapping key, said transferred encrypted private key being decrypted, at the second client, as a function of the obtained wrapping key to obtain the private key.

Claim 21 (currently amended). A computer readable storage medium comprising computer-executable instructions for communicating private data between computers coupled to a data communication network, said computers including a first client and a second client coupled to the data communication network, said computer-readable medium comprising:

first receiving instructions for receiving, at a network server, a plurality of keys encrypted by the first client in response to a request from a user of the first client to roam a private ~~data~~ key, said plurality of keys including the private key, a wrapping key generated by the first client in

response to an encryption password received from the user, and a recovery key generated by the first client, said private key being encrypted ~~by a first client~~ as a function of [[a]] said wrapping key, said wrapping key and said recovery key being unknown to the server, said server ~~and said first client~~ being coupled to the data communication network;

generating instructions for generating, by the server, a backup key in response to the plurality of encrypted keys received from the first client;

storing instructions for storing the received plurality of encrypted ~~private data~~ keys and the generated backup key at the server;

second receiving instructions for receiving, at the server, a request from [[a]] the second client for backup ~~the encrypted private~~ data; and

transferring instructions for transferring the encrypted ~~private data~~ recovery key and the backup key from the server to the second client in response to the received request, said second client generating a backup encrypted recovery key representative of the recovery key encrypted as a function of the transferred backup key ~~for decryption as a function of the wrapping key in response to the received request~~.

Claim 22 (canceled).

Claim 23 (currently amended): The computer readable storage medium of claim [[22]] 21, wherein the transferring instruction includes instruction for transferring the encrypted private key, said encrypted private key being decrypted, at the second client, as a function of the wrapping key, said wrapping key being generated on the second client responsive to the encryption password received from a user of the second client.

Claim 24 (currently amended). The computer readable storage medium of claim [[22]] 21 wherein the first receiving instructions further include instructions for receiving, at the server, the wrapping key encrypted by the first client as a function of a recovery key unknown to the server, said recovery key being generated on the first client in response to a recovery option selected by the user via the first client, and receiving, at the server, the recovery key encrypted by the first client as a function of the wrapping key.

Claim 25 (currently amended). A method of communicating private data between computers coupled to a data communication network, said computers including a first client and a second client coupled to the data communication network, said method comprising:

receiving, at a server, a request from a roaming client for ~~encrypted private~~ backup data, said request including a digest or hashed value of an authentication password, said server ~~and said roaming client~~ being coupled to the data communication network;

determining if a form of the authentication password received from the roaming client is valid;

retrieving, when a form of the authentication password is valid, the ~~encrypted private~~ backup data, said ~~private~~ backup data including a back up key and an encrypted recovery key, said recovery key encrypted as a function of a wrapping key, said wrapping key being previously ~~encrypted~~ generated as a function of an encryption password ~~unknown to the server~~; and

transferring the retrieved encrypted ~~private~~ backup data from the server to the roaming client for generating a backup encrypted recovery ~~decryption as a function of the wrapping~~ key.

Claim 26 (canceled).

Claim 27 (currently amended). The method of claim [[26]] 25, further comprising decrypting the transferred encrypted ~~private~~ recovery key at the roaming client as a function of the wrapping key, said wrapping key being generated on the roaming client in response to the encryption password received from a user of the roaming client.

Claim 28 (currently amended). The method of claim [[27]] 25, further comprising:

~~retrieving the wrapping key encrypted by the home client as a function of a recovery key unknown to the server, said recovery key being generated on the home client in response recovery option selected by the user via the home client;~~

~~retrieving the recovery key encrypted by the home client as a function of the wrapping key;~~

~~decrypting, at the roaming client, the encrypted recovery key as a function of the wrapping key generated on the roaming client to obtain the recovery key;~~

~~retrieving a stored backup key in response to a backup request received from the user of the roaming client, said backup key generated at the server in response to receiving encrypted private data from the home client~~;

~~transferring the backup key from the server to the roaming client via the data communication network in a secure manner in response to the received recovery request, said roaming client encrypting the obtained recovery key as a function of the retreived backup key; and~~

storing, on the roaming client, [[a]] the backup encrypted recovery key representative of the recovery key encrypted as a function of the transferred backup key.

Claim 29 (currently amended). The method of claim [[28]] 25, further comprising:

retrieving the stored backup key in response to a recovery request received from the user of the roaming client, said backup key generated at the server in response to receiving an encrypted private ~~data~~ key from the home client;

transferring the backup key from the server to the roaming client via the data communication network in a secure manner in response to the received recovery request, said roaming client decrypting the backup encrypted recovery key to obtain the recovery key.

Claim 30 (original). The method of claim 29, further comprising transferring the encrypted private key and the encrypted wrapping key from the server to the roaming client in response to the received recovery request, said encrypted wrapping key being decrypted, at the roaming client, as a function of the obtained recovery key to obtain the wrapping key, and said encrypted private key being decrypted, at the roaming client, as a function of the obtained wrapping key to obtain the private key.

Claim 31 (canceled).

Claim 32 (canceled).